(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年2月22日 (22.02.2001)

PCT

(10) 国際公開番号
WO 01/13589 A1

(51) 国際特許分類[7]: H04L 12/56, 12/22, G06F 13/00

(21) 国際出願番号: PCT/JP00/00869

(22) 国際出願日: 2000年2月16日 (16.02.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/231127 1999年8月18日 (18.08.1999) JP

(71) 出願人 および
(72) 発明者: 馬場芳美 (BABA, Yoshimi) [JP/JP]; 〒211-0035 神奈川県横浜市港北区太尾町644 Kanagawa (JP).

(74) 代理人: 佐藤辰彦, 外(SATO, Tatsuhiko et al.); 〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー16階 Tokyo (JP).

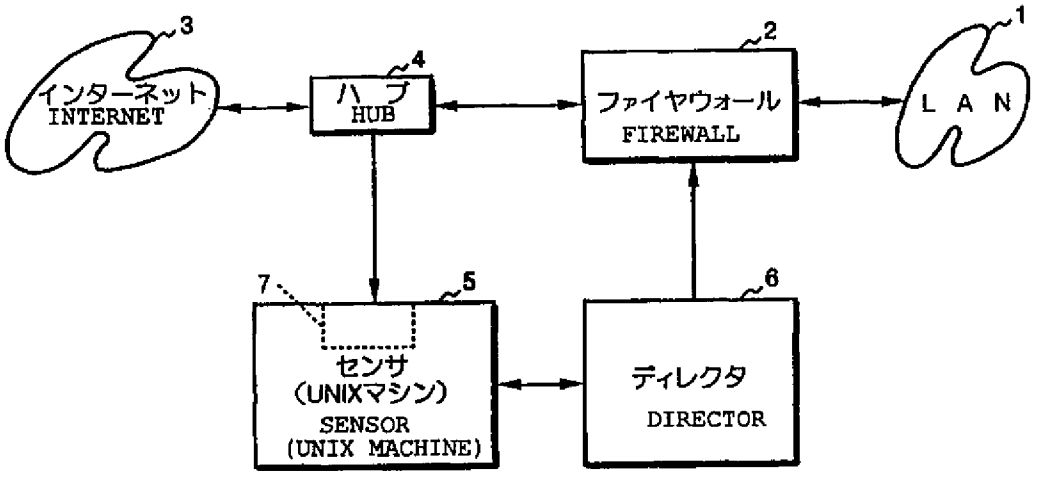
(81) 指定国 (国内): BR, CN, CZ, IL, IN, JP, KR, MX, PL, RU, SG, SK, ZA.

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: CRACKER MONITORING SYSTEM

(54) 発明の名称: クラッカー監視システム



(57) Abstract: A cracker monitoring system has a simplified system configuration for automatically detecting the attacks of a LAN (1) by crackers so that the LAN (1) can be protected from crackers with minimum restrictions of communication without the need for skilled personnel. A sensor (5) is provided at the entrance to the LAN (1) to detect every IP packet passing therethrough. The sensor (5) uses the IP packets to detect various attacks of the LAN (1) by crackers. The information on the attacks detected by the sensor (5) is provided for a director (6) that controls a firewall (2). The director (6) controls the firewall (2) according to the provide information to stop unwelcome IP packets from entering the LAN (1).

[続葉有]

WO 01/13589 A1

(57) 要約:

ＬＡＮ１に対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するＬＡＮ１の保護を図ることができるクラッカー監視システムである。ＬＡＮ１の入り口にそこを通るＩＰパケットを逐次取得するセンサ５を設ける。センサ５は、取得したＩＰパケットに基づき、ＬＡＮ１に対するクラッカーからの各種攻撃を検知する。センサ５が検知した攻撃に関する情報は、ファイヤウォール２を制御するディレクタ６に与えらる。ディレクタ６は与えられた情報に応じてファイヤウォール２の設定を制御し、検知された攻撃に係るＩＰパケットがＬＡＮ１に進入するのを阻止する。

明 細 書

クラッカー監視システム

技術分野

本発明は、クラッカーによるインターネットを介したネットワーク（ＬＡＮ）への攻撃を監視し、さらにはその攻撃からネットワークを保護するためのシステムに関する。

背景技術

近年、企業などの組織内に構築されたネットワーク（ＬＡＮ）は、その多くがインターネットに接続され、他のネットワーク等との間での各種情報のやりとり（通信）がインターネットを介して行われている。この通信では、一般に、所謂ＯＳＩ階層モデルにおけるネットワーク層に主として対応するプロトコルとしてＩＰ（Internet Protocol）が用いられ、通信データはＩＰパケットの形態でやりとりされる。そして、上記ネットワーク層の上位のトランスポート層に主として対応するプロトコル（ＩＰの上位のプロトコル）として、ＴＣＰ（Transmission Control Protocol）あるいはＵＤＰ（User Datagram Protocol）を用いるのが通例である。

この種のネットワークは、インターネット上のサーバや他のネットワークなどとの間で、多種多様な情報のやりとりを低コストで行うことができるという利点を有する。反面、インターネットが極めて高度な公開性を有することから、所謂クラッカーからの攻撃を受ける危険性にさらされることとなる。このため、そのような攻撃からネットワークを保護することが要求される。

このようなネットワークの保護を行うためのシステムとしては、従来、保護しようとするネットワークの入り口に、ファイヤウォール（詳しくはファイヤウォールの機能をもたせたコンピュータ）を設けたシステムが知られている。このファイヤウォールは、あらかじめネットワーク管理者などが定めた種類の通信がネットワーク内とその外部との間で行われるのを阻止し、それ以外の許可された通信のみをネットワーク内とその外部との間で行うことができるようにするものである。この場合、阻止する通信の種類は、例えばＩＰパケットに含まれる送信元ＩＰアドレスや宛先ＩＰアドレス、宛先ポート番号などによって指定可能とされている。

このようなファイヤウォールによれば、ネットワーク内の特定のＩＰアドレスを有するホスト（コンピュータ）、あるいはそのホストの特定のポート番号に対する外部からのアクセスを禁止したり、ネットワークの外部の特定のＩＰアドレス以外のＩＰアドレスからのネットワークへのアクセスを禁止したりすることができる。従って、ネットワークへの進入を禁止する通信データの種類をファイヤウォールに対して適切に設定しておけば、ネットワークへの攻撃の危険性を低減することが可能である。

しかしながら、この種のファイヤウォールでは、その設定を適切に行うためには、通信技術やネットワーク技術、クラッカーによる攻撃手法など、ネットワークに関連した幅広い範囲の技術に対する高度の知識と理解が必要である。さらには、個々のネットワークの構造や運用形態についても熟知している必要がある。

つまり、ファイヤウォールにより阻止する通信の種類は、それにより保護しようとするネットワーク内の各ホストがどのような情報を利用し、もしくは外部に提供し、また、ネットワーク内のどのような情報を保護

すべきか、予想される攻撃としてどのようなものが想定されるか、ということなどを総合的に考慮して決定しなければならない。このためには、ネットワーク関連の高度な熟練技術者を要する。特に、保護しようとするネットワークの規模が比較的大きい場合や、該ネットワークで扱う情報が多岐にわたるような場合には、熟練技術者といえども、ファイヤウォールの適切な設定を行うことは困難である。さらに、ネットワークの構成を変更したような場合や、クラッカーからの攻撃を実際に受けたような場合、あるいは新たな手法の攻撃が出現したような場合には、多くの場合、ファイヤーウォールの設定内容を構築し直す必要がある。このためには、ファイヤウォールを含めたシステムの継続的な運営管理が必要となる。

従って、ファイヤウォールの設定や、その管理運営には、熟練技術者による多大な労力やコストを要するものとなっていた。

また、上記のような従来のファイヤウォールは、攻撃の可能性のある通信をすべて排除しようとするものである。従って、設定により禁止された種類の通信は、その通信がクラッカーからの攻撃によるものであるか否かにかかわらず一律的に排除される。つまり、ネットワークと外部との通信の自由度が必要以上に制限される。このため、ファイヤウォールを備えたネットワークでは、インターネット上の利用可能な情報提供サービスの制限を受ける。この結果、インターネット上の多くの情報資源を有用に享受することができないという不都合を生じるものであった。

本発明はかかる背景に鑑みてなされたものであり、ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができるクラッカー監視システムを提供することを目的とする。

発明の開示

本発明のクラッカー監視システムは、かかる目的を達成するために、ＩＰ（Internet Protocol）に基づく通信を行うネットワークの入り口において該入り口を通過するＩＰパケットを逐次取得して累積的に保持し、保持した複数のＩＰパケットを監視することにより該ネットワークに対するクラッカーからの攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記攻撃を検知したとき、それに応じた所定の処理を行う処理手段とを備えたことを特徴とするものである。

すなわち、本願発明者等がクラッカーによる各種攻撃の手法を検討したところ、一般に、多くの種類の攻撃は、それぞれその攻撃の際に時系列的に通信される複数のＩＰパケットに特徴的な相互関連性を有する。従って、前記ネットワークの入り口で、そこを通過するＩＰパケットを前記攻撃検知手段によって逐次取得して累積的に保持し、その保持した複数のＩＰパケットを監視することで、クラッカーによる前記ネットワークへの攻撃をリアルタイムで検知することができる。そして、このように攻撃を検知できれば、それに応じて前記処理手段により適当な処理（例えばネットワーク管理者などへの報知や、クラッカーによる通信を遮断する処理等）を行うことで、その攻撃からのネットワークの保護を図ることができる。この場合、クラッカーによる攻撃が十分に進行するまでには、一般に長い時間を要する。このため、攻撃が検知された時点、あるいは、それから若干遅れた時点でネットワークを保護するための処置を行っても、ネットワークの損害を十分に抑えることができる。

このような本発明のシステムによれば、クラッカーによる攻撃をリアルタイムで検知できるので、その検知がなされたとき、且つそのときにのみ攻撃に対する対策処置を施せばよい。このため、ネットワーク管理者等は、所謂ログファイル（通信記録簿）等を頻繁に参照したりする必

要性が低減される。さらに、ネットワークの構築や再編等の際に、クラッカーによる攻撃を予測的に考慮するような労力が軽減される。また、攻撃が検知されない通常時は、ネットワークとその外部との通信を、攻撃の可能性を予測して制限する必要性がなく、その通信の自由度を高めることができる。

従って、本発明によれば、ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による労力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができる。

かかる本発明においては、前記攻撃検知手段は、前記ネットワークの入り口を通過する全てのＩＰパケットを受信可能に構成しておく。

これにより、クラッカーによる多くの種類の攻撃を速やかに検知することが可能となる。

さらに、本発明では、前記攻撃検知手段は、ＩＰパケットの受信のみが可能に構成しておく。

これによれば、前記攻撃検知手段は、自己のＩＰアドレスやＭＡＣ（Media Access Control）アドレス等、自己情報のデータをネットワークに送信することがないため、クラッカーなどによりその存在が認識されたり、攻撃の対象とされることがない。従って、攻撃検知手段の安全性を確保し、ひいては、本発明のシステムの信頼性を確保することができる。

また、本発明では、前記攻撃検知手段は、複数の種類の前記攻撃に対して、各種類の攻撃を検知するためのアルゴリズムを保持しており、取得して保持した前記複数のＩＰパケットから前記アルゴリズムに基づき各種類の攻撃を検知する。

これにより、クラッカーによる複数の種類の攻撃を検知することが可

能となり、前記ネットワークの安全性を高めることができる。また、前記アルゴリズムを適宜更新することで、新しい種類の攻撃に対しても対応することが可能となる。

この場合、前記攻撃検知手段は、取得して保持した複数のＩＰパケットを少なくとも送信元ＩＰアドレス及び／又は宛先ＩＰアドレスにより分類する手段を具備し、その分類した複数のＩＰパケットから前記各種類の攻撃を検知する。

すなわち、複数の種類の攻撃を検知するためには、ＩＰパケットの送信元ＩＰアドレスや宛先ＩＰアドレス（これらはＩＰパケットのＩＰヘッダに付与されている）が重要な鍵となることが多い。従って、所定時間内に取得したＩＰパケットを送信元ＩＰアドレス及び／又は宛先ＩＰアドレスにより分類して保持することで、それらのＩＰパケットから攻撃を検知しやすくなる。

本発明では、より具体的には、前記攻撃検知手段は、次のように種々様々の攻撃を検知する。

まず、クラッカーによる第１の種類の攻撃として、一般にポートスキャン（Port Scan）と言われる種類の攻撃がある。この攻撃は、ネットワークに直接的な損害を及ぼすものではないが、その前段階の攻撃として用いられることが多い。この攻撃では、クラッカーは、自身の管理下にあるホストから、攻撃対象のネットワークに対して、パケット内の宛先ＩＰアドレスや宛先ポート番号を適宜変更しながらＩＰパケットを繰り返し送信する。そして、それらのＩＰパケットに対する応答を上記ホストを介して観測する。これにより、攻撃対象のネットワークにおいて、ファイヤウォール等による制限を受けずに外部との通信に利用されているＩＰアドレスやポート番号を探索する。なお、ここで、前記ポート番号は、ＴＣＰあるいはＵＤＰ上で動作するアプリケーションソフト

ウェアのサービス種類（例えば telnet、ftp、smtp、tftp 等）を表すもので、ＩＰパケット内のＴＣＰヘッダあるいはＵＤＰヘッダに付与されるデータである。

この種の攻撃では、上記のようなＩＰパケットの送信は、通常、専用的なツールソフトウェアを用いて行われ、攻撃対象のネットワークには、宛先ＩＰアドレスやポート番号が互いに異なり、且つ送信元ＩＰアドレスが同一であるようなＩＰパケットが比較的短時間内に多数、送信される。

そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数のＩＰパケットであって、少なくともその送信元ＩＰアドレスが互いに同一で且つ宛先ＩＰアドレス又は宛先ポート番号が互いに異なるものが所定数以上あるとき、第１の種類の前記攻撃がなされたことを検知する。

これにより、ポートスキャンと言われる第１の種類の攻撃を確実に検知することができる。

次に、クラッカーによる第２の種類の攻撃として、一般にＳｙｎ－ｆｌｏｏｄと称される種類の攻撃がある。この攻撃は、ＴＣＰの特性を利用してネットワーク内の特定のホストをダウンさせるものである。

すなわち、ＴＣＰでは二つのホスト間で通信を行う場合、まず、両ホスト間で論理的なコネクションの開設処理が行われる。このコネクション開設処理では、一方のホストから他方のホストに対してＳｙｎ用ＩＰパケットを送信する。ここで、該Ｓｙｎ用ＩＰパケットは、それを詳しく言えば、上記一方のホストのＩＰアドレスと他方のホストのＩＰアドレスとをそれぞれ送信元ＩＰアドレス、宛先ＩＰアドレスとしたＩＰパケットで、そのパケット内のＴＣＰヘッダのＳｙｎビット及びＡｃｋビ

ットのうちのＳｙｎビットのみを「１」としたものである。

そして、コネクション開設処理では、このＳｙｎ用ＩＰパケットを受けた他方のホストは、前記一方のホストに対してＳｙｎ／Ａｃｋ用ＩＰパケットを送信する。ここで、該Ｓｙｎ／Ａｃｋ用ＩＰパケットは、詳しくは、上記他方のホストのＩＰアドレスと一方のホストのＩＰアドレスとをそれぞれ送信元ＩＰアドレス、宛先ＩＰアドレスとしたＩＰパケットで、そのパケット内のＴＣＰヘッダのＳｙｎビット及びＡｃｋビットを共に「１」としたものである。

さらに、コネクション開設処理では、このＳｙｎ／Ａｃｋ用ＩＰパケットを受けた前記一方のホストは、前記他方のホストに対してＡｃｋ用ＩＰパケットを送信し、このＡｃｋ用ＩＰパケットを前記他方のホストが受けることで、両ホスト間の論理的なコネクションの開設がなされる。なお、上記Ａｃｋ用ＩＰパケットは、詳しくは、前記Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットで、そのパケット内のＴＣＰヘッダのＳｙｎビット及びＡｃｋビットのうちのＡｃｋビットのみを「１」としたものである。

前記Ｓｙｎ－ｆｌｏｏｄは、このようなＴＣＰの特性を利用する攻撃である。この攻撃では、クラッカーは、攻撃対象のネットワークの特定のホストに対して、比較的短い時間内に多数のＳｙｎ用ＩＰパケットを送信する。そして、それらの各Ｓｙｎ用ＩＰパケットに対して上記特定ホストからＳｙｎ／Ａｃｋ用ＩＰパケットが送信されてきても、Ａｃｋ用ＩＰパケットをその特定ホストに送信しない。このような攻撃がなされたとき、上記特定ホストは、最初に送信されてきたＳｙｎ用ＩＰパケットに対するＳｙｎ／Ａｃｋ用ＩＰパケットを送信した後、所定時間（一般に２分）は、その時間内にＡｃｋ用パケットが送信されてこない限り、そのＡｃｋ用パケットの受信待ち状態となる。そして、この状態

で新たなＳｙｎ用パケットが送信されてくる毎に、上記特定ホストは、新たなＳｙｎ用パケットに応じたコネクション開設処理を順番に完結すべくその新たなＳｙｎ用パケットの情報を通信処理用のバッファ領域に蓄積していく。ところが、バッファ領域の大きさには限界があり、該バッファ領域が満杯になると、前記特定ホストは、ＴＣＰの通信処理やＴＣＰ上のサービス処理を行うことができなくなる。これにより、特定ホストがダウンすることとなる。

この種の攻撃（Ｓｙｎ－ｆｌｏｏｄ）では、前述のように、比較的短い時間内に、比較的多くのＳｙｎ用ＩＰパケットが攻撃対象のネットワーク内の特定のホスト（特定のＩＰアドレスを有するホスト）に対して送信されてくる。また、これに応じて、当該特定のホストからネットワークの外部に向かって、比較的短い時間内に、多くのＳｙｎ／Ａｃｋ用ＩＰパケットが送信される。さらに、それらのＳｙｎ用ＩＰパケットあるいはＳｙｎ／Ａｃｋ用ＩＰパケットに対応して最終的に前記特定ホストに送信されてくるべきＡｃｋ用パケットがその特定ホストに送信されてこない。

そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきたＴＣＰ（Transmission Control Protocol）に基づく複数のＳｙｎ用ＩＰパケットであって、少なくともその宛先ＩＰアドレスが互いに同一であるものが所定数以上あり、且つ、その各Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有すると共に前記ＴＣＰに基づくＡｃｋ用ＩＰパケットが前記所定時間内に取得されていないとき、第２の種類の前記攻撃がなされたことを検知する。

あるいは、前記攻撃検知手段は、取得して保持した前記複数のＩＰパ

ケットのうち、前記ネットワークからその外部に所定時間内に送信されたＴＣＰ（Transmission Control Protocol）に基づく複数のＳｙｎ／Ａｃｋ用ＩＰパケットであって、少なくともその送信元ＩＰアドレスがそれぞれ互いに同一であるものが所定数以上あり、且つ、前記ＴＣＰに基づくＡｃｋ用ＩＰパケットであって、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレス及び宛先ＩＰアドレスとそれぞれ同一の宛先ＩＰアドレス及び送信元ＩＰアドレスを有するものが前記所定時間内に取得されていないとき、第２の種類の前記攻撃がなされたことを検知する。

これにより、Ｓｙｎ－ｆｌｏｏｄといわれる第２の種類の攻撃を確実に検知することができる。

次に、クラッカによる第３の種類の攻撃として、一般にＴｅａｒｄｒｏｐと称される種類の攻撃がある。この攻撃は、ＩＰパケットの分轄（所謂ＩＰフラグメント）に係る処理の特性を利用してネットワーク内の特定のホストをダウンさせるものである。

すなわち、ＩＰパケットは、インターネット上をルータを介して転送される過程で、各ルータのデータ処理容量の関係上、分轄されることがある。また、各ルータにおいてＩＰパケットが転送される際にエラーが生じることもあり、このような場合には、ルータは、ＩＰパケットの再送信を行う。このため、ＩＰパケットの宛先ＩＰアドレスのホストでは、分轄された一部の同じＩＰパケットが、複数受信されるということもある。このようなことから、ＩＰに基づく通信では、最終的にＩＰパケットを受け取るホスト（宛先ＩＰアドレスのホスト）は、受け取ったＩＰパケットが分轄されたものであるとき、残りの全ての分轄部分のＩＰパケットを受信するまで、各分割部分のＩＰパケットを蓄積保持する。そして、全ての分轄部分のＩＰパケットを受信してから、それらを整理し

て元のＩＰパケットのデータを復元する処理を行う。

前記Ｔｅａｒｄｒｏｐは、このようなＩＰパケットの分轄に係る処理の特性を利用する攻撃である。この攻撃では、クラッカーは、比較的短い時間内に、多数の同じ分轄部分のＩＰパケットを攻撃対象のネットワークの特定のホストに送信した上で、残りの分轄部分のＩＰパケットをその特定ホストに送信する。このような攻撃がなされたとき、上記特定ホストは、最終的に残りの分轄部分のＩＰパケットを受信したときに、そのＩＰパケットと、先に送信されてきた多量の分割部分のＩＰパケットとから元のＩＰパケットのデータを復元しようとする処理を行うため、その処理に長時間を要するものとなる。このため、該特定ホストは、事実上、ダウンしてしまうこととなる。

この種の攻撃（Ｔｅａｒｄｒｏｐ）では、前述の如く、比較的短い時間内に、多数の同じ分轄部分のＩＰパケットがネットワーク内の特定のホストに送信されてくる。

そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数の分割されたＩＰパケットであって、同一の分割部分が所定数以上あるとき、第３の種類の前記攻撃がなされていることを検知する。

これにより、Ｔｅａｒｄｒｏｐといわれる第３の種類の攻撃を確実に検知することができる。

次に、クラッカーによる第４の種類の攻撃として、一般にＬａｎｄと称される種類の攻撃がある。この攻撃は、送信元ＩＰアドレス及び宛先ＩＰアドレスが同一であるような、正規にはあり得ないＩＰパケットを、攻撃対象のネットワークの特定のホストに送信する攻撃である。このようなＩＰパケットを送信された特定ホストは、そのＩＰパケットの処理

に手間取ることが多く、ダウンしてしまうことがしばしばある。

この種の攻撃では、上記の如く、送信元ＩＰアドレス及び宛先ＩＰアドレスが同一であるＩＰパケットが、ネットワーク内の特定のホストに送信される。しかも、一般には、そのようなＩＰパケットが比較的短い時間内に、複数、上記特定ホストに送信される。

そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数のＩＰパケットであって、その送信元ＩＰアドレスが宛先ＩＰアドレスと同一のアドレスとなっているものが所定数以上あるとき、第４の種類の前記攻撃がなされていることを検知する。

これにより、Ｌａｎｄとわれる第４の種類の攻撃を確実に検知することができる。

なお、前述したＳｙｎ－ｆｌｏｏｄ、Ｔｅａｒｄｒｏｐ、Ｌａｎｄといわれる攻撃は、一般に、ＤｏＳ（Denial of Service）といわれる種類の攻撃に属するものである。そして、このＤｏＳには、Ｓｙｎ－ｆｌｏｏｄ、Ｔｅａｒｄｒｏｐ、Ｌａｎｄのほかに、例えばＳｍｕｒｆといわれる種類の攻撃や、Ｆｌｏｏｄｉｅといわれる種類の攻撃等もある。本明細書では、ＤｏＳに属する種類の攻撃として、代表的にＳｙｎ－ｆｌｏｏｄ、Ｔｅａｒｄｒｏｐ、Ｌａｎｄを挙げたが、ＳｍｕｒｆやＦｌｏｏｄｉｅ等の攻撃を検知するようにすることも可能である。

次に、クラッカーによる第５の種類の攻撃として、ネットワーク内の特定のホストのユーザのパスワードを獲得する攻撃がある。この攻撃では、クラッカーは、攻撃対象のネットワーク内の特定のホストのユーザ名を使って、telnet等により上記特定ホストにログインし、さらに所定の辞書ファイルなどから選択した多数のパスワードを使って、その特定ホストの操作を試みる。そして、このとき、その特定ホストの操作がで

きるか否かにより、パスワードが判明することとなる。この場合、一般に、ホストに対するパスワードの入力は、無限に（何回でも）試行することができる。このため、クラッカーは、長時間をかければパスワードを獲得することができる。

この種の攻撃では、同一のユーザ名データを含み、しかも互いに異なるパスワードを有する多数のＩＰパケットが、攻撃対象のネットワークの特定ホストに送信される。

そこで、本発明では、取得して保持した前記複数のＩＰパケットのうち、前記ネットワーク内の特定のホストを操作すべく該ネットワークにその外部から所定時間内に送信されてきた複数のＩＰパケットであって、前記特定のホストに係るユーザ名データが互いに同一で、且つパスワードが互いに異なるものが所定数以上あるとき、第５の種類の前記攻撃がなされていることを検知する。

これにより、上記のようにパスワードを獲得する攻撃を確実に検知することができる。

次に、クラッカーによる第６の種類の攻撃として、ネットワーク内の特定のホストに、ネットワーク管理者など、ごく限られた者が、専用のパスワードを入力した状態でしか実行させることができないような処理（所謂、ルートコマンド）を行わせる攻撃がある。この攻撃は、攻撃対象のホストが搭載しているＯＳ（Operating System)のセキュリティホールといわれるバグを利用するものである。

すなわち、例えばＯＳとしてＵＮＩＸ（ＵＮＩＸはＡＴ＆Ｔの登録商標。以下、同じ）を搭載したホストは、バッファオーバフローといわれるセキュリティホールを有している。このセキュリティホールは、例えばプリンタの論理名を表す「ｌｐｒ」に対して比較的大きなデータ（１２８文字以上のデータ）が一度に送られてきたとき、バッファがオーバ

フローし、そのオーバフローしたデータが、ルートコマンドになっていると、ネットワーク管理者などのパスワードが入力されていなくても、そのルートコマンドを実行してしまうというものである。

前記第６の種類の攻撃は、このようなバッファオーバフローといわれるセキュリティホールを攻撃するもので、前述の「ｌｐｒ」に対する所定サイズ以上のデータ列というような、所定のパターンのデータを含むデータ列を有するＩＰパケットがネットワークの特定のホストに送信される。

そこで、本発明では、前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、バッファオーバフローと言われるセキュリティホールを攻撃する所定のパターンのデータを有するデータ列を有するＩＰパケットがあるとき、第６の種類の前記攻撃がなされていることを検知する。

これにより、上記のような第６の種類の攻撃を検知することができる。

前述のようにクラッカーによる攻撃を検知する攻撃検知手段を備えた本発明では、前記処理手段が行う処理は、例えば前記攻撃が検知された旨を表す報知出力を発生する処理である。この報知出力の発生により、ネットワーク管理者やあるいは外部の専門技術者等が、検知された攻撃を排除するための処置を施すことが可能となる。

あるいは、前記処理手段が行う処理は、前記攻撃検知手段が検知した前記攻撃に係る特定の送信元ＩＰアドレス及び／又は宛先ＩＰアドレスを有するＩＰパケットの前記ネットワークへの進入を、前記攻撃を検知してから所定時間阻止する処理である。

これにより、クラッカーによるネットワークへの通信、あるいは、攻撃対象とされたホストへの通信が自動的に遮断され、攻撃の検知に応じたネットワークの保護をリアルタイムで図ることができる。また、前記

攻撃が最後に検知されてから、前記所定時間が経過した後は、前記処理手段による処理の制限を受けずにネットワークと外部との間での自由な通信を再開することが可能となる。

より具体的には、ポートスキャンと言われる前記第１の種類の攻撃を検知したときには、前記処理手段が行う処理は、前記攻撃検知手段が前記第１の種類の攻撃を検知してから所定時間、前記攻撃検知手段が検知した前記第１の種類の攻撃に係る前記送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、前記送信元ＩＰアドレスが、クラッカーがポートスキャンの攻撃に使用しているホストのＩＰアドレスであるので、このＩＰアドレスを送信元ＩＰアドレスとしてネットワークに送信されてくるＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、クラッカーは、攻撃が検知されてから所定時間は、上記送信元ＩＰアドレスのホストからネットワークへの通信を行うことができなくなり、ネットワークに関する情報を取得することができなくなる。なお、このとき、ポートスキャンの攻撃が継続的に行われる限り、逐次、それが検知されるので、その攻撃が継続している間は、事実上、クラッカーは、ネットワークへの通信を行うことができなくなる。

また、Ｓｙｎ－ｆｌｏｏｄといわれる前記第２の種類の攻撃については、この攻撃を前述のようにＳｙｎ用ＩＰパケットに基づいて検知した場合には、前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各Ｓｙｎ用ＩＰパケットと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、前記各Ｓｙｎ用ＩＰパケットの宛先ＩＰアドレスがＳｙｎ

－ｆｌｏｏｄの攻撃の対象とされているホストのＩＰアドレスであるので、そのホストのＩＰアドレスを宛先ＩＰアドレスとするＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。

また、Ｓｙｎ－ｆｌｏｏｄの攻撃をＳｙｎ／Ａｃｋ用ＩＰパケットに基づいて検知した場合には、前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットは、Ｓｙｎ－ｆｌｏｏｄの攻撃を行おうとしているクラッカーの管理下にあるホストからネットワークに送信されてＳｙｎ用パケットに対して、ネットワーク内のホストがクラッカー側に応答するパケットである。従って、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰパケットの送信元ＩＰアドレスが、Ｓｙｎ－ｆｌｏｏｄの攻撃の対象とされているホストのＩＰアドレスである。そこで、そのネットワーク内のホストのＩＰアドレスを宛先ＩＰアドレスとして、ネットワークに送信されたＩＰパケットを該ネットワークに対して遮断する。

上記のように、Ｓｙｎ－ｆｌｏｏｄの攻撃にかかるＩＰパケットがネットワークに進入するのを阻止することで、その攻撃の対象とされたネットワーク内のホストには、所定時間は、Ｓｙｎ用ＩＰパケット等のＩＰパケットが送信されてこなくなる。この場合、攻撃対象とされたホストでは、先に送信されてきたＳｙｎ用ＩＰパケットに対してある程度の時間内（通常２分）にコネクション開設を正常に完結することができないと、自動的にコネクション開設の処理を中止する。従って、上記のようにＩＰパケットが所定時間、送信されてこなくなることで、その所定

時間内に正常状態に復帰することができる。

さらに、本発明では、Ｓｙｎ－ｆｌｏｏｄの検知に応じて、前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含む。

あるいは、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの宛先ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含む。

すなわち、Ｓｙｎ－ｆｌｏｏｄでは、クラッカーがＳｙｎ用ＩＰパケットを送信するに際して、送信元ＩＰアドレスを偽ったり、送信元ＩＰアドレスを適宜変更したりすることもある。しかるに、一般には、前記各Ｓｙｎ用ＩＰパケットの送信元ＩＰアドレス、あるいはそれに対応したＳｙｎ／Ａｃｋ用ＩＰパケットの宛先ＩＰアドレスは、クラッカーの管理下にあるホストのＩＰアドレスである可能性が高い。従って、このようなＩＰアドレスを送信元ＩＰアドレスとして有するＩＰパケットは、攻撃が検知されてから所定時間はネットワークに対して遮断する。これにより、クラッカーの攻撃に対するネットワークの保護をより高めることができる。

この場合さらに、前記各Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレス、あるいは、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの宛先ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記Ｓｙｎ用ＩＰパケットと同一の宛先ＩＰアドレス、あるいは、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩ

Ｐパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定する。

すなわち、Ｓｙｎ－ｆｌｏｏｄの攻撃対象のホストへの通信を遮断する時間（上記の後者側の所定時間）は、該ホストがその攻撃に対して正常に復帰し得る程度の時間で十分である。これに対して、クラッカーの管理下にある可能性の高いホストからネットワークへの通信を遮断する時間（上記の前者側の所定時間）は、ネットワークの保護の観点から、比較的長いものとすることが好ましいと考えられる。従って、上記の前者側の所定時間を、後者側の所定時間よりも長く設定する。

これにより、ネットワーク内のホストの外部との通信の自由度をできるだけ確保しつつ、Ｓｙｎ－ｆｌｏｏｄに対するネットワークの保護も十分に図ることができる。

また、Ｔｅａｒｄｒｏｐといわれる前記第３の種類の攻撃を検知した場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第３の種類の攻撃を検知してから所定時間、前記分割されたＩＰパケットに係る宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、前記分轄されたＩＰパケットに係る宛先ＩＰアドレスが、Ｔｅａｒｄｒｏｐの攻撃の対象とされているホストのＩＰアドレスである。そこで、そのホストのＩＰアドレスを宛先ＩＰアドレスとするＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、Ｔｅａｒｄｒｏｐの攻撃の対象とされたネットワーク内のホストには、所定時間は、分轄されたＩＰパケット等のＩＰパケットが送信されてこなくなる。この場合、攻撃対象とされたホストでは、先に送信されてきた分轄部分のＩＰパケットに対応する残りのＩＰパケットが、ある程度の時間内（通常２分）に受信されないと、そのＩ

Ｐパケットに関する通信処理を自動的に中止する。従って、上記のようにＩＰパケットが所定時間、送信されてこなくなることで、その所定時間内に正常状態に復帰することができる。

さらに、本発明では、Ｔｅａｒｄｒｏｐの検知に応じて、前記処理手段が行う処理は、前記攻撃検知手段が前記第３の種類の攻撃を検知してから所定時間、前記分割されたＩＰパケットに係る送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含む。

すなわち、前述したＳｙｎ－ｆｌｏｏｄの場合と同様に、前記分轄されたＩＰパケットに係る送信元ＩＰアドレスは、クラッカーの管理下にあるホストのＩＰアドレスである可能性が高い。従って、このようなＩＰアドレスを送信元ＩＰアドレスとして有するＩＰパケットは、攻撃が検知されてから所定時間はネットワークに対して遮断する。これにより、クラッカーの攻撃に対するネットワークの保護をより高めることができる。

この場合さらに、前記分割されたＩＰパケットに係る送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記分割されたＩＰパケットに係る宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定する。

すなわち、Ｓｙｎ－ｆｌｏｏｄの場合と同様、Ｔｅａｒｄｒｏｐの攻撃対象のホストへの通信を遮断する時間（上記の後者側の所定時間）は、該ホストがその攻撃に対して正常に復帰し得る程度の時間で十分である。これに対して、クラッカーの管理下にある可能性の高いホストからネットワークへの通信を遮断する時間（上記の前者側の所定時間）は、ネッ

トワークの保護の観点から、比較的長いものとすることが好ましいと考えられる。従って、上記の前者側の所定時間を、後者側の所定時間よりも長く設定する。

これにより、ネットワーク内のホストの外部との通信の自由度をできるだけ確保しつつ、Ｔｅａｒｄｒｏｐに対するネットワークの保護も十分に図ることができる。

また、Ｌａｎｄといわれる前記第４の種類の攻撃を検知した場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第４の種類の攻撃を検知してから所定時間、該第４の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、Ｌａｎｄという攻撃では、送信元ＩＰアドレスと宛先ＩＰアドレスとが同一であるＩＰパケットが送信されてくる。そこで、そのＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、Ｌａｎｄという攻撃からネットワークを保護することができる。

また、ネットワーク内のホストのユーザのパスワードを獲得する前記第５の種類の攻撃を検知する場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第５の種類の攻撃を検知してから所定時間、該第５の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、第５の種類の攻撃に係るＩＰパケットの宛先ＩＰアドレスは、攻撃対象とされたホストのＩＰアドレスである。また、該ＩＰパケットの送信元ＩＰアドレスは、クラッカーの管理下にあるホストのＩＰ

アドレスである。従って、第５の種類の攻撃に係るＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、クラッカーは、種々のパスワードを有するＩＰパケットをネットワークの特定のホストに送信しても、その各パスワードで当該特定ホストを操作することができるのかどうかが判らなくなる。この結果、上記第５の種類の攻撃からネットワークを保護することができる。

また、セキュリティホールを利用した前記第６の種類の攻撃を検知する場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第６の種類の攻撃を検知してから所定時間、該第６の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理である。

すなわち、第６の種類の攻撃に係るＩＰパケットの宛先ＩＰアドレスは、攻撃対象とされたホストのＩＰアドレスである。また、該ＩＰパケットの送信元ＩＰアドレスは、クラッカーの管理下にあるホストのＩＰアドレスである。従って、第６の種類の攻撃に係るＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、クラッカーは、ネットワーク内の特定のホストセキュリティホールを攻撃するＩＰパケットをネットワークの特定のホストに送信しても、該ＩＰパケットは、当該特定ホストに与えられなくなる。この結果、当該特定ホストにルートコマンドを実行させることができなくなり、前記第６の種類の攻撃からネットワークを保護することができる。

また、本発明では、特に、複数種類の攻撃からネットワークを保護する場合に、ＩＰ（Internet Protocol）に基づく通信を行うネットワー

クの入り口において該入り口を通過するＩＰパケットを逐次取得して累積的に保持し、保持した複数のＩＰパケットを該ネットワークに対するクラッカーからの複数種類の攻撃に対応してあらかじめ定めたアルゴリズムにより監視することによって前記複数種類の攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記複数種類の攻撃のうちのいずれかの種類の攻撃を検知したとき、その検知された種類の攻撃に係る特定の送信元ＩＰアドレス及び／又は宛先ＩＰアドレスを有するＩＰパケットの前記ネットワークへの進入を、該攻撃を検知してから所定時間阻止する処理を行う処理手段とを備える。そして、この場合、該処理手段が行う処理に係る前記所定時間は、該攻撃の種類に応じてあらかじめ定めておく。

このように前記攻撃検知手段が検知した種類の攻撃に係る特定の送信元ＩＰアドレス及び／又は宛先ＩＰアドレスを有するＩＰパケットの前記ネットワークへの進入を、該攻撃を検知してから所定時間阻止する処理を行う場合に、その所定時間を攻撃の種類毎に設定しておくこととで、前記特定の送信元ＩＰアドレス及び／又は宛先ＩＰアドレスを有するＩＰパケットの前記ネットワークへの進入を阻止する時間を攻撃の種類毎に必要限に留めることができる。この結果、攻撃が検知されないような状況では、ネットワークと外部との通信を特別な制限を受けずに行なうことができる機会が最大限に多くなり、インターネットを利用した通信の利便性が高まる。

以上説明したように各種の攻撃に係るＩＰパケットのネットワークへの進入を、攻撃の検知に応じて自動的に行う本発明では、前記ネットワークの入り口に、該ネットワークに進入を阻止するＩＰパケットを選択的に設定可能なパケットフィルタを設けておき、前記処理手段は、前記処理を該パケットフィルタを制御することにより行う。

これによれば、前記パケットフィルタとして、例えばファイヤウォー

ルを用いることで、既存のシステムを流用しつつ本発明のシステムを構築することが可能となる。なお、ファイヤウォールよりもＩＰパケットの取捨・選択の機能は劣るが、一般にルータもパケットフィルタとしての機能を有している。従って、前記パケットフィルタとしてルータを用いることも可能である。

図面の簡単な説明

図１は、本発明のクラッカー監視システムの一実施形態のシステム構成図である。

発明を実施するための最良の形態

本発明の一実施形態を図１を参照して説明する。図１は本実施形態のシステム構成図である。

図１において、１はネットワークとしてのＬＡＮである。このＬＡＮ１は、例えばイーサネット（Ethernet）を用いて構築されたものであり、図示を省略する複数のホスト（コンピュータ）がイーサネット・ケーブルやハブ等を介して接続されている。各ホストには、それをイーサネット・ケーブルに接続するイーサネット・カードや、ＴＣＰ／ＩＰの処理を行うためのソフトウェア、ＴＣＰ／ＩＰ上で機能する各種アプリケーションソフトウェア（例えば、telnet、ftp、smtp 等）が実装され、ＩＰに基づく通信を可能としている。

なお、ＬＡＮ１は、イーサネット上で構築されたものに限らず、トークンリング等、他の形態で構築されたものであってもよい。

本実施形態のシステムでは、ＬＡＮ１の入り口に、パケットフィルタとしてのファイヤウォールの機能をもたせたコンピュータ２（以下、このコンピュータ２を単にファイヤウォール２と称する）が設けられてい

る。そして、ＬＡＮ１はファイヤウォール２を介してインターネット３に接続されている。ファイヤウォール２は、どのような種類のＩＰパケットのＬＡＮ１への進入を禁止するかを規定するデータが書き込まれるファイル（以下、フィルタ設定ファイルという）を有している。そして、ファイヤウォール２は、このフィルタ設定ファイルで、ＬＡＮ１への進入が禁止された種類のＩＰパケットがインターネット３側から送信されてきたときに、そのＩＰパケットを廃棄してＬＡＮ１への進入を阻止する。また、フィルタ設定ファイルで、ＬＡＮ１への進入が禁止されていないＩＰパケットが送信されてきたときには、それをＬＡＮ１に転送する。

ファイヤウォール２とインターネット３との間には、ハブ４が介装され、このハブ４に攻撃検知手段の機能をもたせたセンサ５が接続されている。また、このセンサ５には、前記ファイヤウォール２を制御する処理手段の機能を有するディレクタ６が接続されている。これらのセンサ５及びディレクタ６はそれぞれコンピュータにより構成されたものである。

前記センサ５は例えばＵＮＩＸマシンにより構成され、イーサネットカード７を介して前記ハブ４に接続されている。この場合、センサ５には、ｔｃｐｄｕｍｐといわれるソフトウェアが実装されている。このｔｃｐｄｕｍｐによって、ハブ４を通る全てのＩＰパケットをイーサネットカード７を介して取得する（ヒアリングする）ことができる。このような動作は、プロミス・キャス・モード（promise cast mode）といわれることが多い。そして、センサ５は、取得した各ＩＰパケットをその取得時点の時刻データと共に図示しないハードディスクに記憶保持するようにしている。なお、ハードディスクに記憶保持したＩＰパケットの総量が所定の許容量に達したときには、センサ５は、最も古いＩＰパ

ケットを消去し、新たに取得されたＩＰパケットをハードディスクに記憶保持する。

また、センサ５は、ＩＰアドレスを持たず、ＡＲＰ（Adress Resolution Protocol)や、ＲＡＲＰ（Reverse Adress Resolution Protocol）のパケット等、応答を促すパケットが送信されてきても、それに対する応答をしないようにソフトウェア的に設定されている。つまり、センサ５はＩＰパケットの受信（取り込み）のみを行うことできるものとされている。

さらに、センサ５には、前述した第１～第６の種類の攻撃を検知するためのソフトウェア（以下、攻撃検知アルゴリズム）が実装されている。なお、この攻撃検知アルゴリズムは、ディレクタ６に実装しておき、該ディレクタ６とのデータ授受を行いつつ該攻撃検知アルゴリズムの処理をセンサ５に行わせるようにしてもよい。

前記ディレクタ６には、前記ファイヤウォール２を制御するソフトウェア（以下、フィルタ制御アルゴリズムという）が実装されている。この場合、フィルタ制御アルゴリズムは、センサ５により検知される攻撃に応じて、前記フィルタ設定ファイルのデータを適宜書き換えることで、前記ファイヤウォール２を制御するものである。

次に、かかる本実施形態の作動を説明する。

前記センサ５は、取得されるＩＰパケットを前述の如くハードディスクに記憶保持しつつ、所定のサイクルタイム毎に次のような処理を行う。すなわち、センサ５は、ハードディスクから所定の時間間隔分の複数のＩＰパケットを、送信元ＩＰアドレス及び宛先ＩＰアドレスの値別に分類した上で、図示しないメモリに取り込んで保持する。つまり、所定の時間間隔分の複数のＩＰパケットのうち、同一の送信元ＩＰアドレスを有するものをひとまとめにすると共に、同一の宛先ＩＰアドレスを有す

ものをひとまとめにして、メモリに取り込む（以下の説明では、このようにひとまとめにされたＩＰパケットの組をＩＰパケット群という）。そして、このメモリに取り込んだ複数のＩＰパケットに対して、後述する攻撃検知の処理を行った上で、それらのＩＰパケットをメモリから消去する。

この場合、各サイクルタイムにおいて、メモリに取り込むＩＰパケットは、前回のサイクルタイムでメモリに取り込んだＩＰパケットのうちの最も古いＩＰパケットの取得時刻から所定時間を経過した時刻以後に取得されたものである。

各サイクルタイムにおけるセンサ５による攻撃検知の処理は、攻撃検知アルゴリズムに従って次のように行われる。

センサ５は、まず、前記第１～第６の種類の攻撃のうち、例えば、第１の種類の攻撃、すなわちポートスキャンを検知する処理を行う。この処理では、センサ５は、メモリに前述のように取り込んだＩＰパケットのうち、送信元ＩＰアドレスが同一で、且つ該送信元ＩＰアドレスがＬＡＮ１の外部のものである各ＩＰパケット群に対し、その各ＩＰパケット群に含まれるＩＰパケットが有する全ての宛先ＩＰアドレスの値（これはＬＡＮ１に属するＩＰアドレスの値である）を抽出する。そして、上記の各ＩＰパケット群で抽出した宛先ＩＰアドレスの各値に対し、そのＩＰパケット群（同一の送信元ＩＰアドレスのＩＰパケット群）から、該宛先ＩＰアドレスの値と同一の宛先ＩＰアドレスを有し、且つＴＣＰヘッダあるいはＵＤＰヘッダ内の宛先ポート番号が互いに異なり、且つ、連続した所定時間内（例えば３０秒内）に取得されたＩＰパケットの個数をカウントする。

このとき、このカウント数が所定数（例えば２０個）に達した場合には、センサ５は、ポートスキャンの攻撃がなされていることを検知する。

そして、そのことを示すデータと、この攻撃が検知されたＩＰパケット群の送信元ＩＰアドレスの値データとを（以下、これらのデータを第１種攻撃検知データという）前記ディレクタ６に与える。

このような処理が送信元ＩＰアドレスが同一で、且つ該送信元ＩＰアドレスがＬＡＮ１に属さない全てのＩＰパケット群に対し順次行われる。

なお、本実施形態におけるポートスキャンの検知では、ポート番号が互いに異なるＩＰパケットの個数をカウントするようにしたが、次のような処理によりポートスキャンを検知するようにしてもよい。すなわち、送信元ＩＰアドレスが同一で、且つ、該送信元ＩＰアドレスがＬＡＮ１外部のものである各ＩＰパケット群に対し、その各ＩＰパケット群に含まれるＩＰパケットが有する全ての宛先ポート番号の値を抽出する。さらに、その抽出した宛先ポート番号の各値に対し、該宛先ポート番号を抽出したＩＰパケット群から、該宛先ポート番号の値と同一の宛先ポート番号を有し、且つ宛先ＩＰアドレスが互いに異なり、且つ、連続した所定時間内に取得されたＩＰパケットの個数をカウントする。そして、そのカウント数が所定数に達した場合にポートスキャンが行われていることを検知する。

一方、センサ５から前述のような第１種攻撃検知データを与えられた前記ディレクタ６は、該第１種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば５分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、ポートスキャンの攻撃からＬＡＮ１が保護される。

なお、ディレクタ６は、上記所定時間（５分間）が経過するまでの間に、先に与えられた第１種攻撃検知データと同一の第１種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（５分間）、該第１種攻撃検知データの送信元ＩＰアドレスからのＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、ポートスキャンの攻撃が続いている限り、その送信元ＩＰアドレスからのＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（５分間）が経過するまでに、前記第１種攻撃検知データが与えられなかった場合には、その第１種攻撃検知データの送信元ＩＰアドレスからのＩＰパケットのＬＡＮ１への進入の阻止を解除する。

前述のようにポートスキャンの攻撃の検知処理を行ったセンサ５は、次に、第２の種類の攻撃（Ｓｙｎ－ｆｌｏｏｄ）の検知処理を行う。

この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、該ＩＰパケット群に含まれるＳｙｎ用ＩＰパケットをその取得時刻順に順次抽出する。そして、抽出した各Ｓｙｎ用ＩＰパケットの取得時刻から所定時間（例えば２秒間）内に取得されたＳｙｎ用ＩＰパケットが、同じ宛先ＩＰアドレスのＩＰパケット群内に存在するか否か調べる。そして、そのようなＳｙｎ用ＩＰパケットが存在する場合には、先に抽出したＳｙｎ用ＩＰパケットを含めてそれらのＳｙｎ用ＩＰパケットの個数をカウントする。さらに、そのカウントしたそれぞれのＳｙｎ用ＩＰパケットに対して、それぞれに対応するＡｃｋ用ＩＰパケット（詳しくは該Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレスを有し、且つ、該Ｓｙｎ用ＩＰパケットのＴＣＰヘッダ中のシーケンス番号の次のシーケンス番号を有するＡｃｋ用ＩＰパケット）であって、且つ該Ｓ

ｙｎ用ＩＰパケットの取得時刻から上記所定時間（２秒間）内に取得されたものが、同じ宛先ＩＰアドレスのＩＰパケット群内に存在するか否かを調べる。このとき、そのようなＡｃｋ用ＩＰパケットが存在する場合には、その都度、上記のカウント数を「１」づつ減少させる。そして、最終的に、対応するＡｃｋ用ＩＰパケットの存在を調べ終わったときに上記のカウント数が所定数（例えば１６個）以上である場合には、Ｓｙｎ－ｆｌｏｏｄの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＳｙｎ用ＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第２種攻撃検知データという）前記ディレクタ６に与える。

このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。

なお、本実施形態では、Ｓｙｎ用ＩＰパケットの個数に基づいてＳｙｎ－ｆｌｏｏｄを検知したが、次のような処理によりＳｙｎ－ｆｌｏｏｄを検知するようにしてもよい。すなわち、送信元ＩＰアドレスが同一で且つ、該送信元ＩＰアドレスがＬＡＮ１に属する各ＩＰパケット群に対し、該ＩＰパケット群に含まれるＳｙｎ／Ａｃｋ用ＩＰパケットをその取得時刻順に順次抽出する。そして、抽出した各Ｓｙｎ／Ａｃｋ用ＩＰパケットの取得時刻から所定時間（例えば２秒間）内に取得されたＳｙｎ／Ａｃｋ用ＩＰパケットが、同じ送信元ＩＰアドレスのＩＰパケット群内に存在するか否か調べる。このとき、そのようなＳｙｎ／Ａｃｋ用ＩＰパケットが存在する場合には、先に抽出したＳｙｎ／Ａｃｋ用ＩＰパケットを含めてそれらのＳｙｎ／Ａｃｋ用ＩＰパケットの個数をカウントする。さらに、そのカウントしたそれぞれのＳｙｎ／Ａｃｋ用ＩＰパケットに対して、該Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスのＩＰパケット群を調べる。このとき、

該Ｓｙｎ／Ａｃｋ用ＩＰパケットに対応するＡｃｋ用ＩＰパケット（詳しくは該Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有し、且つ、該Ｓｙｎ／Ａｃｋ用ＩＰパケットのＴＣＰヘッダ中のシーケンス番号の次のＡｃｋ番号を有するＡｃｋ用ＩＰパケット）であって、且つ該Ｓｙｎ／Ａｃｋ用ＩＰパケットの取得時刻から上記所定時間（２秒間）内に取得されたものが、当該ＩＰパケット群内に存在するか否かを調べる。そして、そのようなＡｃｋ用パケットが存在する場合には、その都度、上記のカウント数を「１」づつ減少させる。そして、最終的に、対応するＡｃｋ用ＩＰパケットの存在を調べ終わったときに上記のカウント数が所定数（例えば１６個）以上である場合には、Ｓｙｎ－ｆｌｏｏｄの攻撃がなされていることを検知する。

なお、この場合にセンサ５からディレクタ６に与えるデータは、Ｓｙｎ－ｆｌｏｏｄの攻撃を検知したことを示すデータと、上記Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データである。この場合、Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データは、それぞれ、先に説明した前記第２種攻撃検知データにおけるＳｙｎ用ＩＰパケット宛先ＩＰアドレスの値データ、送信元ＩＰアドレスの値データに相当するものである。

一方、センサ５から前述のような第２種攻撃検知データを与えられた前記ディレクタ６は、該第２種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば２分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。同時に、ディレクタ６は、第２種攻撃検知データに含まれる宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現

在から所定時間（例えば２秒間）阻止するようにファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレスを有するＩＰパケット、あるいは上記宛先ＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、Ｓｙｎ－ｆｌｏｏｄの攻撃からＬＡＮ１が保護されると共に、この攻撃の対象とされていたＩＰアドレスのホストがダウンせずに正常状態に復帰することができる。

なお、ポートスキャンの検知時の場合と同様、ディレクタ６は、第２種攻撃検知データにおける送信元ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（２分間）が経過するまでの間に、先に与えられた第２種攻撃検知データと同一の第２種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（２分間）、該第２種攻撃検知データの送信元ＩＰアドレスからのＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。このことは、第２種攻撃検知データにおける宛先ＩＰアドレスを有するＩＰパケットの排除についても同様である。従って、Ｓｙｎ－ｆｌｏｏｄの攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレスからのＩＰパケット、あるいはその攻撃に係る宛先ＩＰアドレスへのＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、第２種攻撃検知データにおける送信元ＩＰアドレスを有するＩＰパケットの排除と、第２種攻撃検知データにおける宛先ＩＰアドレスを有するＩＰパケットの排除とのいずれについても、それぞれに対応する上記所定時間（２分間、２秒間）が経過するまでに、前記第２種攻撃検知データが与えられなかった場合には、その第２種攻撃検知データの送信元ＩＰアドレスを有するＩＰパケット、あるいは、第２種攻撃検知データの宛先ＩＰアド

レスを有するＩＰパケットのＬＡＮ１への進入の阻止を解除する。

前述のようにＳｙｎ－ｆｌｏｏｄの攻撃の検知処理を行ったセンサ５は、次に、第３の種類の攻撃（Ｔｅａｒｄｒｏｐ）の検知処理を行う。

この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、該ＩＰパケット群に含まれる分轄されたＩＰパケット（以下、単に、分轄パケットという）を順次抽出する。この場合、ＩＰでは、分轄パケットは、そのＩＰヘッダ中の特定のフラグが「１」となっているか、もしくは、フラグメントオフセットといわれるデータが「０」より大きな値となっている。これにより、分轄パケットを見出すことができる。そして、センサ５は、抽出した各分轄パケットの取得時刻から所定時間（例えば５分間）内に取得され、且つ、該分轄パケットとＩＰヘッダ中のＩＰ識別番号及びフラグメントオフセットの値がそれぞれ同一であるもの（抽出した分轄パケットと同一の分轄パケット）が、該分轄パケットと同じＩＰパケット群内にあるかを調べる。このとき、そのような分轄パケットがある場合には、先に抽出した分轄パケットを含めてそれらの分轄パケットの個数をカウントする。そして、このカウント数が所定数（例えば８０個）以上である場合には、Ｔｅａｒｄｒｏｐの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知された分轄パケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第３種攻撃検知データという）前記ディレクタ６に与える。

このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。

一方、センサ５から前述のような第３種攻撃検知データを与えられた前記ディレクタ６は、前記Ｓｙｎ－ｆｌｏｏｄが検知された場合と全く

同じやり方で、ファイヤーウォール制御する。すなわち、第３種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（２分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。同時に、第３種攻撃検知データに含まれる宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（２秒間）阻止するようにファイヤウォール２のフィルタ設定ファイルを書き換える。

これにより、Ｔｅａｒｄｒｏｐの攻撃からＬＡＮ１が保護されると共に、この攻撃の対象とされていたＩＰアドレスのホストがダウンせずに正常状態に復帰することができる。

上記のようにＴｅａｒｄｒｏｐの攻撃の検知処理を行ったセンサ５は、次に、第４の種類の攻撃（Ｌａｎｄ）の検知処理を行う。

この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群から、該ＩＰパケット群の宛先ＩＰアドレスと同じ値の送信元ＩＰアドレスを有するＩＰパケットを抽出する。さらに、その抽出したＩＰパケットと同じ宛先ＩＰアドレスのＩＰパケット群の中から、該ＩＰパケットと同じ送信元ＩＰアドレスを有し、且つ該ＩＰパケットの取得時刻から所定時間（例えば２分間）内に取得されたＩＰパケットが存在するか否かを調べる。そして、そのようなＩＰパケットが存在する場合には、先に抽出したＩＰパケットを含めてそれらのＩＰパケットの該ＩＰパケットの個数をカウントする。このとき、該カウント数が所定数（例えば６個）以上である場合には、Ｌａｎｄの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＩＰパケットの送信元ＩＰアドレスの値データを（以下、これらのデータを第４種攻撃検

知データという）前記ディレクタ６に与える。

このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。

一方、センサ５から前述のような第４種攻撃検知データを与えられた前記ディレクタ６は、第４種攻撃検知データに含まれる送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有し、且つ、該送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば３分間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、Ｌａｎｄの攻撃からＬＡＮ１が保護される。

この場合、ポートスキャンの検知時の場合と同様、ディレクタ６は、第４種攻撃検知データにおける送信元ＩＰアドレスと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（６分間）が経過するまでの間に、先に与えられた第４種攻撃検知データと同一の第４種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（６分間）、該第４種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、Ｌａｎｄの攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（６分間）が経過するまでに、前記第４種攻撃検知データが与えられなかった場合には、その第４種攻撃検知データの送信元ＩＰアドレスと同一の送信元

ＩＰアドレス及び宛先ＩＰアドレス有するＩＰパケットのＬＡＮ１への進入の阻止を解除する。

なお、本実施形態では、第４種攻撃検知データとして、Ｌａｎｄの攻撃に係るＩＰパケットの送信元ＩＰアドレスの値データをディレクタ６に与えるようにしたが、Ｌａｎｄの攻撃に係るＩＰパケットの送信元ＩＰアドレスと、宛先ＩＰアドレスとは同じ値である。従って、その送信元ＩＰアドレスの値データの代わりに、宛先ＩＰアドレスの値をディレクタ６に与えてもよいことはもちろんである。

前述のように、Ｌａｎｄの攻撃の検知処理を行ったセンサ５は、次に第５の種類の攻撃（パスワードの獲得）を検知する処理を行う。

この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、ＬＡＮ１のホストのユーザ名データ及びパスワードデータを含むＩＰパケットを抽出する。それらの抽出したＩＰパケットの中から、ユーザ名データが同一で、且つ、パスワードデータが互いに異なり、且つ、連続した所定時間（例えば２分間）内に取得されたＩＰパケットの個数をカウントする。このとき、このカウント数が所定数（例えば２０個）以上であれば、クラッカーがパスワードを獲得するための第５の種類の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第５種攻撃検知データという）前記ディレクタ６に与える。

このような処理が宛先ＩＰアドレスが同一で、且つ該宛先ＩＰアドレスがＬＡＮ１に属する全てのＩＰパケット群に対して順次行われる。

一方、センサ５から前述のような第５種攻撃検知データを与えられた前記ディレクタ６は、該第５種攻撃検知データの送信元ＩＰアドレス及

び宛先ＩＰアドレスとそれぞれ同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば１時間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレス及びＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、パスワードの獲得を狙った第５の種類の攻撃からＬＡＮ１が保護される。

なお、ポートスキャンの検知時の場合と同様、ディレクタ６は、第５種攻撃検知データにおける送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（１時間）が経過するまでの間に、先に与えられた第５種攻撃検知データと同一の第５種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（１時間）、該第５種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入を阻止するようにファイヤウォール２を制御する。従って、第５の種類の攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（１時間）が経過するまでに、前記第５種攻撃検知データが与えられなかった場合には、その第５種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入の阻止を解除する。

前述のように、第５の種類の攻撃の検知処理を行ったセンサ５は、次に第６の種類の攻撃（セキュリティホールの攻撃）を検知する処理を行う。

この処理では、センサ５は、宛先ＩＰアドレスが同一であるＩＰパケ

ット群のうち、ＬＡＮ１に属する宛先ＩＰアドレスの各ＩＰパケット群に対し、例えばプリンタの論理名である「ｌｐｒ」を有し、且つ、データサイズが１２８文字以上であるＩＰパケットを検索する。そして、そのようなＩＰパケットが見つかった場合には、ＬＡＮ１のホストのスルーホールを攻撃する第６の種類の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたＩＰパケットの送信元ＩＰアドレスの値データ及び宛先ＩＰアドレスの値データとを（以下、これらのデータを第６種攻撃検知データという）前記ディレクタ６に与える。

一方、センサ５から前述のような第６種攻撃検知データを与えられた前記ディレクタ６は、該第６種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスとそれぞれ同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットがＬＡＮ１に進入するのを現在から所定時間（例えば４時間）阻止するように前記ファイヤウォール２のフィルタ設定ファイルを書き換える。このとき、ファイヤウォール２は、上記送信元ＩＰアドレス及びＩＰアドレスを有するＩＰパケットがインターネット３から送信されてくると、そのＩＰパケットを廃棄し、ＬＡＮ１への進入を阻止する。これにより、ＬＡＮ１のホストのスルーホールを攻撃する第６の種類の攻撃からＬＡＮ１が保護される。

なお、ポートスキャンの検知時の場合と同様、ディレクタ６は、第６種攻撃検知データにおける送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットの排除に係る上記所定時間（４時間）が経過するまでの間に、先に与えられた第６種攻撃検知データと同一の第５種攻撃検知データがセンサ５から再度与えられれば、その時点から上記所定時間（４時間）、該第６種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットのＬＡＮ１への進入を阻止するように

ファイヤウォール２を制御する。従って、第６の種類の攻撃が続いている限り、その攻撃に係る送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットは、ＬＡＮ１に進入することはできない。そして、ディレクタ６は、上記所定時間（４時間）が経過するまでに、前記第６種攻撃検知データが与えられなかった場合には、その第５種攻撃検知データの送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットＩＰパケットのＬＡＮ１への進入の阻止を解除する。

以上説明したようにして、本実施形態のシステムによれば、センサ５や、ディレクタ６を導入するだけで、クラッカーによるＬＡＮ１への各種の攻撃をリアルタイムで検知しつつ、検知された攻撃からＬＡＮ１を保護する適正な処置を自動的に迅速に施すことができる。このため、ネットワーク管理者等は、クラッカーによる攻撃を考慮してＬＡＮ１を構築したり、頻繁にログファイルを参照したりする労力が大幅に削減され、ひいては、ＬＡＮ１の維持管理のコストを低減することができる。また、クラッカーによる各種攻撃をリアルタイムで検知できることから、攻撃が検知されない状況では、ＬＡＮ１と外部との通信を格別に制限する必要性が少なくなる。このため、通常時は、ＬＡＮ１の通信の自由度を高めることができ、インターネット３上の情報資源を有用に活用することができる。

なお、以上説明した実施形態では、ＬＡＮ１の入り口にファイヤウォール３を設けておき、クラッカーによる攻撃が検知されてとき、該ファイヤウォール３を制御することで、検知された攻撃を自動的に排除する処置を行った。但し、クラッカーによる攻撃が検知されたときに、単に、その旨の報知をネットワーク管理者や、専門の警備管理者等に行うようにしてもよい。

この場合には、例えば前記ディレクタ６あるいはセンサ５を公衆回線

や専用回線を介してネットワーク管理者や、警備管理者等のホストに接続しておく。そして、攻撃が検知された場合に、前述した第１乃至第６種攻撃検知データのような情報をネットワーク管理者や警備管理者等のホストにディレクタ６あるいはセンサ５から送信する。このようにしたときには、検知された攻撃からＬＡＮ１を保護するための具体的な処置は、ネットワーク管理者等が直接的に行うこととなる。しかるに、この場合であっても、ネットワーク管理者等は、上記の報知を受けたときに処置を施せばよく、しかも攻撃の種類は検知されるので、攻撃に対する処置を比較的容易に施すことができる。

また、前記実施形態では、第１乃至第６の種類の攻撃を順番に検知するものを示したが、それらの攻撃の検知処理を並列的に行うようにすることも可能である。

また、前記実施形態では、前述したＤｏＳ（Denial of Service）に属する攻撃のうち、Ｓｙｎ－ｆｌｏｏｄ、Ｔｅａｒｄｒｏｐ、Ｌａｎｄを検知するものを示した。但し、この他にも、ＳｍｕｒｆやＦｌｏｏｄｉｅといわれるような攻撃を検知するようにすることも可能である。

産業上の利用可能性

以上のように、本発明のクラッカー監視システムは、企業や官庁等の組織に構築されたＬＡＮ等のネットワークをクラッカーによる攻撃から簡易に保護し、また、その保護を通信の自由度を必要以上に損なうことなく行うことができるシステムとして有用である。

請 求 の 範 囲

1．ＩＰ（Internet Protocol）に基づく通信を行うネットワークの入り口において該入り口を通過するＩＰパケットを逐次取得して累積的に保持し、保持した複数のＩＰパケットを監視することにより該ネットワークに対するクラッカーからの攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記攻撃を検知したとき、それに応じた所定の処理を行う処理手段とを備えたことを特徴とするクラッカー監視システム。

2．前記攻撃検知手段は、前記ネットワークの入り口を通過する全てのＩＰパケットを受信可能に構成されていることを特徴とする請求の範囲第１項記載のクラッカー監視システム。

3．前記攻撃検知手段は、ＩＰパケットの受信のみが可能に構成されていることを特徴とする請求の範囲第 2 項記載のクラッカー監視システム。

4．前記攻撃検知手段は、複数の種類の前記攻撃に対して、各種類の攻撃を検知するためのアルゴリズムを保持しており、取得して保持した前記複数のＩＰパケットから前記アルゴリズムに基づき各種類の攻撃を検知することを特徴とする請求の範囲第１項記載のクラッカー監視システム。

5．前記攻撃検知手段は、取得して保持した複数のＩＰパケットを少なくとも送信元ＩＰアドレス及び／又は宛先ＩＰアドレスにより分類する手段を具備し、その分類した複数のＩＰパケットから前記各種類の攻撃を検知することを特徴とする請求の範囲第４項記載のクラッカー監視システム。

6．前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数のＩＰパケットであって、少なくともその送信元ＩＰアドレスが互い

に同一で且つ宛先ＩＰアドレス又は宛先ポート番号が互いに異なるものが所定数以上あるとき、第１の種類の前記攻撃がなされたことを検知することを特徴とする請求の範囲第１項記載のクラッカー監視システム。

７．前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきたＴＣＰ（Transmission Control Protocol）に基づく複数のＳｙｎ用ＩＰパケットであって、少なくともその宛先ＩＰアドレスが互いに同一であるものが所定数以上あり、且つ、その各Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有すると共に前記ＴＣＰに基づくＡｃｋ用ＩＰパケットが前記所定時間内に取得されていないとき、第２の種類の前記攻撃がなされたことを検知することを特徴とする請求の範囲第１項記載のクラッカー監視システム。

８．前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークからその外部に所定時間内に送信されたＴＣＰ（Transmission Control Protocol）に基づく複数のＳｙｎ／Ａｃｋ用ＩＰパケットであって、少なくともその送信元ＩＰアドレスがそれぞれ互いに同一であるものが所定数以上あり、且つ、前記ＴＣＰに基づくＡｃｋ用ＩＰパケットであって、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレス及び宛先ＩＰアドレスとそれぞれ同一の宛先ＩＰアドレス及び送信元ＩＰアドレスを有するものが前記所定時間内に取得されていないとき、第２の種類の前記攻撃がなされたことを検知することを特徴とする請求の範囲第１項記載のクラッカー監視システム。

９．前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数の分割されたＩＰパケットであって、同一の分割部分が所定数以上あるとき、第３の種類の前記攻撃がなされていることを検知することを特

徴とする請求の範囲第１項記載のクラッカー監視システム。

１０．前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワークにその外部から所定時間内に送信されてきた複数のＩＰパケットであって、その送信元ＩＰアドレスが宛先ＩＰアドレスと同一のアドレスとなっているものが所定数以上あるとき、第４の種類の前記攻撃がなされていることを検知することを特徴とする請求の範囲第１項記載のクラッカー監視システム。

１１．前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、前記ネットワーク内の特定のホストを操作すべく該ネットワークにその外部から所定時間内に送信されてきた複数のＩＰパケットであって、前記特定のホストに係るユーザ名データが互いに同一で、且つパスワードが互いに異なるものが所定数以上あるとき、第５の種類の前記攻撃がなされていることを検知することを特徴とする請求の範囲第１項記載のクラッカー監視システム。

１２．前記攻撃検知手段は、取得して保持した前記複数のＩＰパケットのうち、バッファオーバフローと言われるセキュリティホールを攻撃する所定のパターンのデータを有するデータ列を有するＩＰパケットがあるとき、第６の種類の前記攻撃がなされていることを検知することを特徴とする請求の範囲第１項記載のクラッカー監視システム。

１３．前記処理手段が行う処理は、前記攻撃が検知された旨を表す報知出力を発生する処理であることを特徴とする請求の範囲第１項記載のクラッカー監視システム。

１４．前記処理手段が行う処理は、前記攻撃検知手段が検知した前記攻撃に係る特定の送信元ＩＰアドレス及び／又は宛先ＩＰアドレスを有するＩＰパケットの前記ネットワークへの進入を、前記攻撃を検知してから所定時間阻止する処理であることを特徴とする請求の範囲第１項記載

のクラッカー監視システム。

１５．前記処理手段が行う処理は、前記攻撃検知手段が前記第１の種類の攻撃を検知してから所定時間、前記攻撃検知手段が検知した前記第１の種類の攻撃に係る前記送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第６項記載のクラッカー監視システム。

１６．前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各Ｓｙｎ用ＩＰパケットと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第７項記載のクラッカー監視システム。

１７．前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求の範囲第１６項記載のクラッカー監視システム。

１８．前記各Ｓｙｎ用ＩＰパケットと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記各Ｓｙｎ用ＩＰパケットと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求の範囲第１７項記載のクラッカー監視システム。

１９．前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケット

が前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第８項記載のクラッカー監視システム。

２０．前記処理手段が行う処理は、前記攻撃検知手段が前記第２の種類の攻撃を検知してから所定時間、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの宛先ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求の範囲第１９項記載のクラッカー監視システム。

２１．前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの宛先ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記各Ｓｙｎ／Ａｃｋ用ＩＰパケットの送信元ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求の範囲第２０項記載のクラッカー監視システム。

２２．前記処理手段が行う処理は、前記攻撃検知手段が前記第３の種類の攻撃を検知してから所定時間、前記分割されたＩＰパケットに係る宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第９項記載のクラッカー監視システム。

２３．前記処理手段が行う処理は、前記攻撃検知手段が前記第３の種類の攻撃を検知してから所定時間、前記分割されたＩＰパケットに係る送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求の範囲第２２項記載のクラッカー監視システム。

２４．前記分割されたＩＰパケットに係る送信元ＩＰアドレスと同一の送信元ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入す

るのを阻止する前記所定時間は、前記分割されたＩＰパケットに係る宛先ＩＰアドレスと同一の宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求の範囲第２３項記載のクラッカー監視システム。

２５．前記処理手段が行う処理は、前記攻撃検知手段が前記第４の種類の攻撃を検知してから所定時間、該第４の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第１０項記載のクラッカー監視システム。

２６．前記処理手段が行う処理は、前記攻撃検知手段が前記第５の種類の攻撃を検知してから所定時間、該第５の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第１１項記載のクラッカー監視システム。

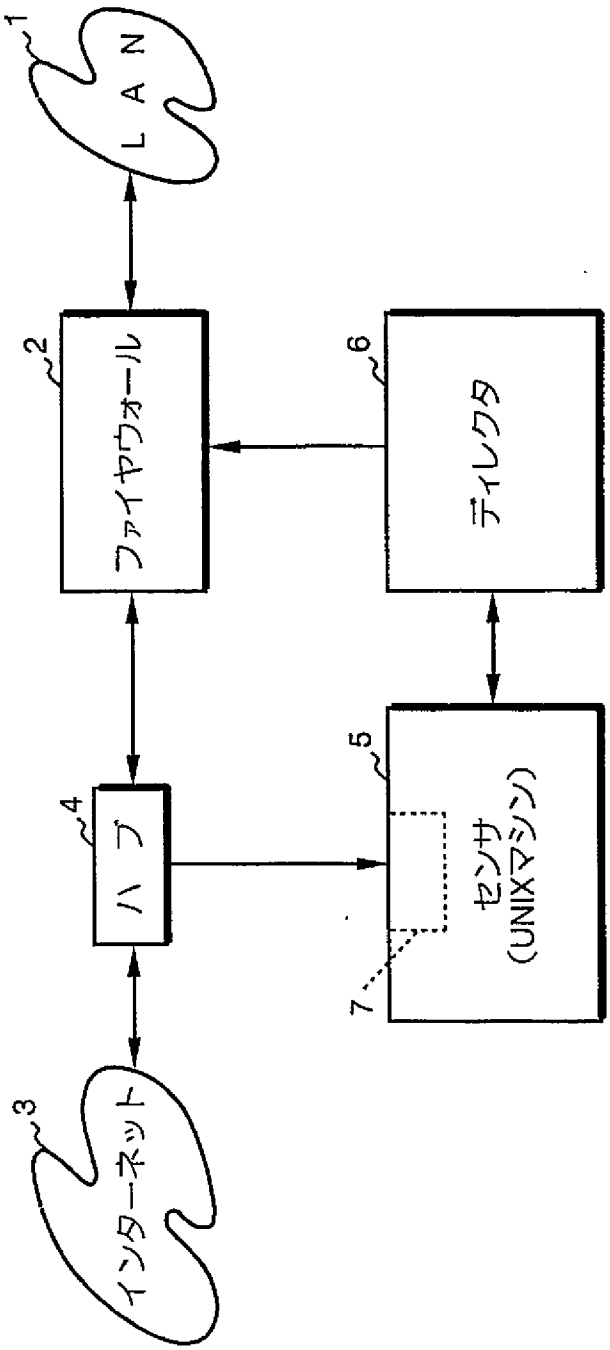
２７．前記処理手段が行う処理は、前記攻撃検知手段が前記第６の種類の攻撃を検知してから所定時間、該第６の種類の攻撃に係る前記ＩＰパケットと同一の送信元ＩＰアドレス及び宛先ＩＰアドレスを有するＩＰパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求の範囲第１２項記載のクラッカー監視システム。

２８．ＩＰ（Internet Protocol）に基づく通信を行うネットワークの入り口において該入り口を通過するＩＰパケットを逐次取得して累積的に保持し、保持した複数のＩＰパケットを該ネットワークに対するクラッカーからの複数種類の攻撃に対応してあらかじめ定めたアルゴリズムにより監視することによって前記複数種類の攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記複数種類の攻撃のうちのいずれかの種類の

攻撃を検知したとき、その検知された種類の攻撃に係る特定の送信元ＩＰアドレス及び／又は宛先ＩＰアドレスを有するＩＰパケットの前記ネットワークへの進入を、該攻撃を検知してから所定時間阻止する処理を行う処理手段とを備え、該処理手段が行う処理に係る前記所定時間は、該攻撃の種類に応じてあらかじめ定められていることを特徴とするクラッカー監視システム。

２９．前記ネットワークの入り口には、該ネットワークに進入を阻止するＩＰパケットを選択的に設定可能なパケットフィルタが設けられ、前記処理手段は、前記処理を該パケットフィルタを制御することにより行うことを特徴とする請求の範囲第１４項～第２８項のいずれか１項に記載のクラッカー監視システム。

FIG. 1



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/00869

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L 12/56
H04L 12/22
G06F 13/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L 12/56
H04L 12/22
G06F 13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho (Y1,Y2) 1926-1996 Toroku Jitsuyo Shinan Koho(U) 1994-2000
Kokai Jitsuyo Shinan Koho (U) 1971-2000 Jitsuyo Shinan Toroku Koho(Y2)1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JOIS (HACKER+CRACKER+HACKING+CRACKING+ILLEGAL ACCESS)*PACKET (in Japanese)
http://www.cert.org/
http://www.jpcert.or.jp/

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Yasushi SAKAKIBARA,"Survey Security Shindan, Kanshi Tool", Nikkei Open System, No. 65, (Japan), Nikkei BP K.K., (15.08.98), pp.130-132	1-5,13,14,29 6-12,15-17, 19,20,22,23, 25-27
A		18,21,24,28
Y	"Security Kyouka wo hakarou -Part 1 Network to Security", UNIX USER, Vol.7, No.10, (Japan), Softbank K.K., (01.10.98), pp. 51-56	6,12,15,27
Y	Hideyuki YAMADA, "Firewall no Kiso Chishiki to VPN no Koukatekina Riyouhou wo osaeru", Nikkei Open System, No.63, (Japan), Nikkei BP K.K., (15.06.98), pp.266-273	7-9,16,17, 19,20,22,23
Y	IP Denial-of-Service Attacks, CERT Advisory, CA-97.28, (USA), (26.05.98), Full text	10,25
Y	D.B.Chapman,E.D.Zwicky,"Firewall Kouchiku: Internet Security", 1st edition, 3rd printing, (Japan),	11,26

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 May, 2000 (08.05.00)	16 May, 2000 (16.05.00)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/00869

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Kabushiki Kaisha Orairi, Japan, (15.07.97), p.426	
A	Masahiro KUSUNOKI, et al., "Crack Bougyo Nuumon (the 1st volume)", DOS/V magazine, Vol.8, No.1 (Japan), Softbank K.K., (01.01.99), pp.266-270	1-29
A	TCP SYN Flooding and IP Spoofing Attacks, CERT Advisory, CA-96.21,(USA),(24.08.98), Full text	1-29
A	Yousuke TAKEI et al., "Traffic Pattern wo mochiita Fusei Access Kenshutsu Houshiki", Tsuushin Society Meeting in 1999, B-7-46, of the Institute of Electronics, Information and Communication Engineers the Institute of Electronics, Information and Communication Engineers, (Japan),(16.08.99), p.86	1-29
P,A	Yousuke TAKEI et al., "Traffic Pattern wo mochiita Fusei Access Kenshutsu oyobi Tsuiseki Houshiki", Technical Research Report (IN99-75), of the Institute of Electronics, Information and Communication Engineers Vol. 99, No.436, The Institute of Electronics, Information and Communication Engineers, (Japan), (13.12.99), pp.37-42	1-29

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／００８６９

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ⁷ Ｈ０４Ｌ　１２／５６
Ｈ０４Ｌ　１２／２２
Ｇ０６Ｆ　１３／００

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ⁷ Ｈ０４Ｌ　１２／５６
Ｈ０４Ｌ　１２／２２
Ｇ０６Ｆ　１３／００

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報（Ｙ１，Ｙ２）　１９２６－１９９６年
日本国公開実用新案公報（Ｕ）　１９７１－２０００年
日本国登録実用新案公報（Ｕ）　１９９４－２０００年
日本国実用新案登録公報（Ｙ２）　１９９６－２０００年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
ＪＯＩＳ　（ハッカー+クラッカー+ハッキング+クラッキング+不正アクセス）*パケット
http://www.cert.org/
http://www.jpcert.or.jp/

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	日経オープンシステム，第６５号，（日）， 日経ＢＰ社，（１５．０８．９８）， 榊原康，「サーベイ　セキュリティ診断・監視ツール」， 第１３０－１３２頁	１－５， １３，１４， ２９
Ｙ		６－１２， １５－１７， １９，２０， ２２，２３， ２５－２７
Ａ		１８，２１， ２４，２８

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０８．０５．００	１６．０５．００

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	吉田　隆之	５Ｘ　２９４７
	電話番号　０３－３５８１－１１０１　内線　３５９４	

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＵＮＩＸ　ＵＳＥＲ，第７巻第１０号，（日），ソフトバンク株式会社，（０１．１０．９８），「セキュリティ強化を図ろうーPart1　ネットワークとセキュリティ」，第５１－５６頁	６，１２，１５，２７
Ｙ	日経オープンシステム，第６３号，（日），日経ＢＰ社，（１５．０６．９８），山田英之，「ファイアウオールの基礎知識とＶＰＮの効果的な利用法を押さえる」，第２６６－２７３頁	７－９，１６，１７，１９，２０，２２，２３
Ｙ	IP Denial-of-Service Attacks, CERT Advisory, CA-97.28, (米)，（２６．０５．９８），全文	１０，２５
Ｙ	D. B. Chapman, E. D. Zwicky,「ファイアウォール構築　インターネット・セキュリティ」，初版第３刷，（日），株式会社オライリー・ジャパン，（１５．０７．９７），第４２６頁	１１，２６
Ａ	ＤＯＳ／Ｖ　ｍａｇａｚｉｎｅ，第８巻第１号，（日），ソフトバンク株式会社，（０１．０１．９９），楠正宏，田口篤，「クラック防御入門前編」，第２６６－２７０頁	１－２９
Ａ	TCP SYN Flooding and IP Spoofing Attacks, CERT Advisory, CA-96.21, (米)，（２４．０８．９８），全文	１－２９
Ａ	１９９９年電子情報通信学会通信ソサイエティ大会，Ｂ－７－４６，電子情報通信学会，（日），（１６．０８．９９），武井洋介，太田耕平，加藤寧，グレン マンスフィールド，根元義章，「トラヒックパターンを用いた不正アクセス検出方式」，第８６頁	１－２９
Ｐ，Ａ	電子情報通信学会技術研究報告（ＩＮ９９－７５），第９９巻第４３６号，電子情報通信学会，（日），（１３．１２．９９），武井洋介，太田耕平，加藤寧，グレン　マンスフィールド，根元義章，「トラヒックパターンを用いた不正アクセス検出及び追跡方式」，第３７－４２頁	１－２９